



Configuring FortiOS v5.0 Webfiltering for HTTPS scanning without SSL Deep Scanning

Introduction

The FortiOS FortiGuard Webfiltering and URL Filter can be configured to block or allow HTTPS websites without the need of SSL Deep Inspection. The webfilter daemon has the ability to extract the website's hostname from the SSL Certificate (CN field), which is sent via an unencrypted session (HTTP) before the SSL tunnel is established, and it uses this hostname info to rate the website (not the full URL), thus blocking or allowing access.

Since SSL Deep Inspection is not necessary, there's no need of installing the Fortigate's self-signed certificate in all workstations or buying a valid certificate for that purpose.

Configuration

1. Create a new SSL/SSH Inspection profile and enable HTTPS over port 443.

Enable	Protocol	Inspection Port(s)
<input checked="" type="checkbox"/>	HTTPS	443
<input type="checkbox"/>	SMTPS	465
<input type="checkbox"/>	POP3S	995
<input type="checkbox"/>	IMAPS	993
<input type="checkbox"/>	FTPS	990

2. Unset the option *Scan Encrypted Connection* under your Webfilter Profile.

FortiGate VM64

Edit Web Filter Profile

Comments: default web filtering 21/255

Inspection Mode: ☒ Proxy ☐ Flow-based ☐ DNS

☒ FortiGuard Categories

Show All

- ☒ Local Categories
- ☒ Potentially Liable
- ☒ Adult/Mature Content
- ☒ Bandwidth Consuming
- ☒ Security Risk
- ☒ General Interest - Personal
- ☒ General Interest - Business
- ☒ Unrated

Quota on Categories with Monitor, Warning and Authenticate Actions

☐ Enable Safe Search

☐ Scan Encrypted Connections

☐ Enable Web Site Filter

☐ Web Resume Download Block

☐ Block Invalid URLs

☒ HTTP POST Action: Comfort

☐ Remove Java Applet Filter

☐ Remove ActiveX Filter

☐ Remove Cookie Filter

☐ Log all search keywords

☐ Allow Blocked Override

☐ Provide Details for Blocked HTTP 4xx and 5xx Errors

☐ Rate Images by URL (Blocked images will be replaced with blanks)

☐ Web Content Filter

☐ Allow Websites When a Rating Error Occurs

☐ Rate URLs by Domain and IP Address

☐ Block HTTP Redirects by Rating

Apply

This is the same of running the following CLI commands:

```
config webfilter profile
  edit <profile_name>
    set options https-url-scan
  end
end
```

3. Select both SSL/SSH Inspection and Webfilter profiles on your policy that controls HTTPS access.

The screenshot shows the 'New Policy' configuration window in FortiOS. The left sidebar has 'Policy' selected. The main configuration area is for a policy of subtype 'Address'. The 'Incoming Interface' is 'port1', 'Source Address' is 'all', 'Outgoing Interface' is 'port2', 'Destination Address' is 'all', 'Schedule' is 'always', 'Service' is 'ALL', and 'Action' is 'ACCEPT'. Under 'Logging Options', 'Log Security Events' is selected. Under 'Security Profiles', 'Web Filter' and 'SSL/SSH Inspection' are both set to 'ON' and are highlighted with red boxes. Other profiles like AntiVirus, Application Control, and IPS are set to 'OFF'. 'Proxy Options' is set to 'default'.

When configuring the FGT to do this if a webpage is blocked, by default the FGT will send a replacement-message to the user and since it is a HTTPS website, the replacement-message URL will also be via HTTPS. In this case the user will also be asked to accept the FGT's self-signed certificate, but THIS IS ONLY for the replacement-message URL and it does not mean SSL Deep Scanning is enabled.

You can easily test this accessing an allowed HTTPS website and you will see that it won't ask you to accept the FGT's self-signed certificate, while for a blocked website you'll see the certificate warning message on your browser.

There's a CLI command that can disable the replacement-message for HTTPS websites and the browser's time-out message will be showed instead:

```
config webfilter profile
  edit "default"
    set https-replacemsg disable
  end
end
```